On Critical Exponents of Matroids and Linear Codes (Designs, Codes, Graphs and Related Areas)

Shiromoto, Keisuke

数理解析研究所講究録
第 1889 巻 2014 年 7-12

On Critical Exponents of Matroids and Linear Codes

Keisuke Shiromoto (keisuke@kumamoto-u.ac.jp)
Department of Mathematics and Engineering,
Kumamoto University,
2-39-1, Kurokami, Kumamoto 860-8555, Japan

Abstract

The critical exponent of a matroid is one of the important parameters in matroid theory which is related to the critical problem (cf. [6]). A representable matroid over $GF(q)$ is corresponding to a linear code over $GF(q)$. In this note, we give a bound on critical exponents of linear codes and give a construction of linear codes which attain the equality of the bound.

1 Preliminaries

Let E be a finite set and $\rho : 2^E \to \mathbb{Z}^+ \cup \{0\}$ be a function. $M = (E, \rho)$ is called a *matroid* if M has the following properties:

(R1) If $X \subseteq E$, then $0 \leq \rho(X) \leq |X|$.

(R2) If $X \subseteq Y \subseteq E$, then $\rho(X) \leq \rho(Y)$.

(R3) If X and Y are subsets of E, then

$$\rho(X \cup Y) + \rho(X \cap Y) \leq \rho(X) + \rho(Y).$$

We refer the reader to [9] and [11] for the basic definitions in matroid theory.

For a matroid $M = (\rho, E)$, the *characteristic polynomial* $p(M; \lambda)$ of M is defined by

$$p(M; \lambda) = \sum_{X \subseteq E} (-1)^{|X|} \lambda^{\rho(E) - \rho(X)}.$$

Let M be a matroid representable over $GF(q) = \mathbb{F}_q$. It is well known that $p(M; q^k) \geq 0$, for all $k \in \mathbb{Z}^+$. Then the *critical exponent* $c(M; q)$ of M is defined by

$$c(M; q) = \begin{cases} \infty, & \text{if } M \text{ has a loop;} \\ \min\{j \in \mathbb{Z}^+ : p(M; q^j) > 0\}, & \text{otherwise.} \end{cases}$$

Thus if M has no loops, then $p(M;q^k) > 0$ for all $k \geq c(M;q)$. For a matroid M which is representable over $\mathbb{F}_q$, one of the critical problems is the problem of determining the critical exponent $c(M;q)$ (cf. [6, 1]). However, this is difficult in general.

The *support* and *weight* of each vector $\boldsymbol{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$ is given by

$$\begin{aligned} \operatorname{supp}(\boldsymbol{x}) &:= \{ i \ : \ x_i \neq 0 \} ; \\ \operatorname{wt}(\boldsymbol{x}) &:= |\operatorname{supp}(\boldsymbol{x})| . \end{aligned}$$

Similarly, the *support* and *weight* of each subset $B \subseteq \mathbb{F}_q^n$ are defined as follows:

$$\begin{aligned} \operatorname{Supp}(B) &:= \bigcup_{\boldsymbol{x} \in B} \operatorname{supp}(\boldsymbol{x}) ; \\ \operatorname{wt}(B) &:= |\operatorname{Supp}(B)| . \end{aligned}$$

Let C be an $[n,k]$ code over $\mathbb{F}_q$, that is, a k-dimensional subspace of the vector space $\mathbb{F}_q^n$. Let G be a generator matrix of C, that is, a $k \times n$ matrix over $\mathbb{F}_q$ whose rows form a basis for C. Set $E := \{1, 2, \ldots, n\}$. For each subset $X \subseteq E$, the *punctured code*, denoted by $C \setminus X$, is the linear code obtained by deleting the coordinate X from each codeword in C. It is easy to check that if we define a function ρ by $\rho(X) = \dim C \setminus (E - X)$, for any $X \subseteq E$, then $M_C = (E, \rho)$ is a matroid, conversely, if M is a representable matroid over $\mathbb{F}_q$, then there exists a linear code C such that $M = M_C$ (cf. [11, 9]). Thus, for an $[n,k]$ code over $\mathbb{F}_q$, the *characteristic polynomial* $p(C;\lambda)$ of C is defined by

$$p(C;\lambda) = \sum_{X \subseteq E} (-1)^{|X|} \lambda^{k - \dim C \setminus X},$$

and the *critical exponent* $c(C;q)$ of C is defined by

$$c(C;q) = \begin{cases} \infty, & \text{if } \operatorname{Supp}(C) \neq E; \\ \min\{ j \in \mathbb{Z}^+ \ : \ p(C;q^j) > 0 \}, & \text{otherwise.} \end{cases}$$

For any subset $X \subseteq E$, the *shortened code*, denoted by C/X, is the linear code obtained by deleting the (zero) coordinates X from each codewords $\boldsymbol{x} \in C$ with $\operatorname{supp}(\boldsymbol{x}) \cap X = \emptyset$. Crapo and Rota ([4]) prove the following theorem widely known as the *Critical Theorem* (cf. Theorem 2 in [1]).

Lemma 1 (The Critical Theorem) *Let C be an $[n,k]$ code over $\mathbb{F}_q$. For any $X \subseteq E$ and any $m \in \mathbb{Z}^+$, the number of ordered m-tuples $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m)$ of codewords $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m$ in C with $\operatorname{supp}(\boldsymbol{v}_1) \cup \cdots \cup \operatorname{supp}(\boldsymbol{v}_m) = X$ is $p(C/X;q^m)$.*

From Lemma 1, if there exists at least one set of m codewords $V = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m\}$ in C with $\operatorname{Supp}(V) = E$, then $p(C;q^m) > 0$ and so $c(C;q) \leq m$. For $0 \leq r \leq k$ and any $X \subseteq E$, let $A_X^{(r)}$ be the number of r-dimensional subcodes D of C with $\operatorname{Supp}(D) = X$. We note that the polynomial

$$W_C^{(r)}(x,y) = \sum_{i=0}^{n} A_i^{(r)} x^{n-i} y^i$$

is the r-th *support weight enumerator* of C, where $A_i^{(r)} \sum_{X \in \binom{E}{i}} A_X^{(r)}$ (cf. [5]).

Then we have the following result:

Proposition 2 *Let C be an $[n,k]$ code over $\mathbb{F}_q$ having generator matrix G and set $E = \{1,2,\ldots,n\}$. The following are equivalent:*

(1) $c(C;q) = m$.

(2) $\min\{r : 0 \le r \le k,\ A_E^{(r)} \neq 0\} = m$.

(3) *m is the smallest positive integer such that there exists a $(k-m)$-dimensional subspace U of $\mathbb{F}_q^k$ which does not contain any of the n column vectors of G.*

2 Bounds on Critical Exponents

Let G be a $k \times n$ matrix over $\mathbb{F}_q$ which contains as columns exactly one multiple of each nonzero vector in $\mathbb{F}_q^k$. Then the $[n = (q^k-1)/(q-1), k]$ code C having generator matrix G is a dual Hamming code and $C^\perp$ is a $[n, n-k, 3]$ Hamming code. It is also known that, for any r, $1 \le r \le k$,

$$\sum_{X \in \binom{E}{i}} A_X^{(r)} = \begin{cases} \begin{bmatrix} k \\ r \end{bmatrix}_q & i = (q^k - q^{k-r})/(q-1), \\ 0 & \text{otherwise,} \end{cases}$$

where $\begin{bmatrix} k \\ r \end{bmatrix}_q$ denotes the Gaussian binomial coefficient (cf. [5]). So we have that $i = n$ if and only if $r = k$.

Proposition 3 *If C is a dual Hamming $[n,k]$ code over $\mathbb{F}_q$, then*

$$\min\{r : 0 \le r \le k,\ A_E^{(r)} \neq 0\} = k.$$

A *maximum distance separable* (MDS) code over $\mathbb{F}_q$ is an $[n,k]$ code over $\mathbb{F}_q$ whose minimum Hamming weight is $n-k+1$. According to Theorem 6, p. 321, in [7], the number A_w of codewords of weight w in an MDS $[n,k]$ code over $\mathbb{F}_q$ is given by

$$A_w = \binom{n}{w}(q-1)\sum_{j=0}^{w-d}(-1)^j\binom{w-1}{j}q^{w-d-j}, \tag{1}$$

for $d \le w \le n$, where $d = n-k+1$.

Theorem 4 *Let C be an MDS $[n,k]$ code over $\mathbb{F}_q$. Then*

$$c(C;q) \le 2.$$

Remark 5 From Proposition 3, for a $[q+1, 2]$ MDS code C over $\mathbb{F}_q$, we have that $c(C;q) = 2$. So the bound is sharp.

It is known that a uniform matroid $U_{n,m}$ representable over $\mathbb{F}_q$ is corresponding to a matroid obtained by an MDS $[n,m]$ code over $\mathbb{F}_q$ (cf. [9]). As a corollary of the above theorem, we have the following.

Corollary 6

$$c(U_{n,m}; q) \leq 2.$$

In general, we have the following bound on critical exponents for linear codes over finite fields.

Theorem 7 *Let C be an $[n, k]$ code over $\mathbb{F}_q$ having generator matrix G. If $d^{\perp} > q$, then*

$$c(C; q) \leq k - d^{\perp} + 2,$$

except when C is a binary codes such that $d^{\perp} = n$ is odd or such that $n = 2^k - 1$ and $d^{\perp} = 3$ in which case $c(C; q) = k - d^{\perp} + 3$, where $C^{\perp}$ denotes the minimum Hamming weight of the dual code $C^{\perp}$.

As a corollary of the above theorem, we have the following bound on critical exponents for representable matroids over finite fields.

Corollary 8 *Let M be a rank k representable simple matroid over $\mathbb{F}_q$ with girth g. If $g > q$, then*

$$c(M; q) \leq k - g + 2,$$

except when M is a binary matroid isomorphic to $U_{2l+1,2l}$ or $PG(k-1, 2)$ in which case $c(M; q) = k - g + 3$.

Example 9 Let C be the ternary $[11, 5]$ code having generator matrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 2 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 2 & 1 \\ 0 & 0 & 1 & 0 & 0 & 2 & 1 & 2 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 2 & 2 & 2 & 1 & 0 & 1 \end{pmatrix}.$$

Then the dual code $C^{\perp}$ is an $[11, 6, 5]$ quadratic residue code. By a Magma calculation, we have that

$$A_E^{(1)} = 0,\ A_E^{(2)} = 330,\ A_E^{(3)} = 825,\ A_E^{(4)} = 110,\ A_E^{(5)} = 1,$$

where $E = \{1, 2, \ldots, 11\}$. If M_C is the vector matroid obtained from G, then $c(M_C; 3) = 2(= 5 - 5 + 2)$ and so M_C holds the equality in Theorem 7.

3 A construction of tangential blocks

As defined in [3, 6], for $1 \leq r \leq k - 1$, a set M of points of the projective geometry $PG(k-1, q)$ is an *r-block* over $\mathbb{F}_q$ if every $(k-r)$-dimensional subspace in $PG(k-1, q)$ contains at least one point in M. If X is a flat in M, a *tangent* of X is a $(k-r)$-dimensional subspace U in $PG(k-1, q)$ such that

$$M \cap U = X.$$

An r-block M is called to be *minimal* if every point in M has a tangent, and to be *tangential* if every proper nonempty flat in M of rank not exceeding $k - r$ has a tangent.

Alternatively, a matroid M is a *tangential r-block* over $\mathbb{F}_q$ if the following conditions hold:

(i) M is simple and representable over $\mathbb{F}_q$.

(ii) $p(M; q^r) = 0$.

(iii) $p(M/F; q^r) > 0$ whenever F is a proper nonempty flat of M.

Proposition 10 *For any positive integer k, set $K := \{1, 2, \ldots, k\}$. For an m $(1 \leq m \leq k)$, we take an m elements subset $T \in \binom{K}{m}$ and a family $\mathcal{V}$ of $(m-1)$ distinct points $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_{m-1} \in PG(k-1, q)$ with $\mathrm{supp}(\boldsymbol{v}_i) \cap T = \emptyset$, $i = 1, 2, \ldots, m-1$. Define*

$$\begin{aligned} X^T &:= \{\boldsymbol{x} \in PG(k-1,q) \ : \ \mathrm{supp}(\boldsymbol{x}) \cap T = \emptyset\}, \\ Y^T_{\mathcal{V}} &:= \{\boldsymbol{x} \in PG(k-1,q) \ : \ |\mathrm{supp}(\boldsymbol{x}) \cap T| = 1\} \setminus \{\boldsymbol{v}_i + \lambda \boldsymbol{e}_j \ : \ \boldsymbol{v}_i \in \mathcal{V},\ \lambda \in \mathbb{F}_q - \{0\},\ j \in T\}, \\ Z^T &:= \{\boldsymbol{x} \in PG(k-1,q) \ : \ \mathrm{supp}(\boldsymbol{x}) \in \binom{T}{2}\}. \end{aligned}$$

Then $M := X^T \cup Y^T_{\mathcal{V}} \cup Z^T$ is a $(k-m)$-block over $\mathbb{F}_q$.

Then we can give a construction of tangential blocks as follows:

Theorem 11 *Let M be the set of points in $PG(k-1,q)$ defined in Proposition 10. If $m - 1 \leq q^{k-m-1}$, then M is a tangential $(k-m)$-block over $GF(q)$.*

From the definition, M is a minimal r-block over $\mathbb{F}_q$ if and only if $c(C; q) = r + 1$ for the linear code having generator matrix G whose column vectors are all points in M (cf. p. 168 in [3]).

Corollary 12 *Let M be the set of points defined in Proposition 10. If $m = 2$, then the linear code C over $\mathbb{F}_q$ whose generator matrix obtained from M attains the bound in Theorem 7.*

Proof. From the definition of M, it finds that $d^{\perp} = 3$, since there exist three column vectors in G which are linearly dependent. Thus we have that

$$k - 2 + 1 = k - 1 = c(C; q) \leq k - 3 + 2 = k - 1.$$

$\square$

Example 13 Let C be the binary $[22, 5]$ code over $\mathbb{F}_q$ having generator matrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

From Theorem 11, G forms a binary tangential 3-block. Moreover, we have that

$$\begin{aligned} p(M_C; \lambda) &= \lambda^5 - 22\lambda^4 + 175\lambda^3 - 610\lambda^2 + 9 - 4\lambda - 448 \\ &= (\lambda - 1)(\lambda - 2)(\lambda - 4)(\lambda - 7)(\lambda - 8). \end{aligned}$$

If M_C is the vector matroid obtained from G, then $c(M_C; 2) = 4 (= 5 - 3 + 2)$ and so M_C holds the equality in Theorem 7.

References

[1] T. Britz, Extensions of the critical theorem, *Discrete Mathematics* **305** (2005), pp.55–73.

[2] T. Britz, Higher support matroids, *Discrete Mathematics* **307** (2007), pp.2300–2308.

[3] T. Brylawski and J. Oxley, The Tutte polynomial and its applications; *Matroid applications*, pp. 123–225, Cambridge Univ. Press, Cambridge, 1992.

[4] H. Crapo and G.-C. Rota, *On the Foundations of Combinatorial Theory: Combinatorial geometries*, MIT Press, Cambridge, MA, London, 1970 (Preliminary Edition).

[5] T. Kløve, Support weight distribution of linear codes, *Discrete Mathematics* **106/107** (1992), pp. 311–316.

[6] J. P. S. Kung, Critical problems, in: *Matroid Theory*, Seattle, WA, 1995, *Contemporary Mathematics*, **197**, American Mathematical Society, Providence, RI, 1996, pp. 1–127.

[7] F. J. MacWilliams and N. J. A. Sloane, *TheTheory of Error-Correcting Codes*, Amsterdam, The Netherlands: North-Holland, 1977.

[8] J. Oxley, Colouring, packing and the critical problem, *Quart. J. Math. Oxford* (2), **29** (1978), pp. 11–22.

[9] J. Oxley, *Matroid Theory*, Oxford University Press, New York, 1992.

[10] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, 2003.

[11] D. J. A. Welsh, *Matroid Theory*, Academic Press, London, 1976.